Memorandum of Understanding

between:

The Information Commissioner

for

The United Kingdom of Great Britain & Northern Ireland

- and -

The New Zealand Department of Internal Affairs

for Cooperation in the Regulation of Unsolicited Electronic Messages

1. Introduction

1.1 This Memorandum of Understanding ("**MoU**") establishes a framework for cooperation between

(I) The Information Commissioner (the "**Commissioner**") and

(II) The Department of Internal Affairs ("**Internal Affairs**"),

together referred to as the "**Participants**".

1.2 The Participants recognise the nature of the modern global economy, including the increased reliance on electronic means to carry out commercial activities, the increase in circulation and exchange of personal data across borders, the increasing complexity of information technologies, and the resulting need for increased cross-border enforcement cooperation.

1.3 The Participants acknowledge that they have similar functions and duties in relation to unsolicited marketing compliance in their respective countries.

1.4 This MoU reaffirms the intent of the Participants to deepen their existing relations and to promote exchanges to assist each other in the enforcement of laws relating to unsolicited electronic messaging.

1.5 This MoU sets out the broad principles of cooperation and collaboration between the Participants and the legal framework governing the sharing of relevant information and intelligence between them, excluding always the sharing of personal information.

1.6 The Participants confirm that nothing in this MoU should be interpreted as imposing a requirement on the participants to co-operate with each other. In particular, there is no requirement to co-operate in circumstances which would breach their legal responsibilities, including:

(a) in the case of the Commissioner: The Data Protection Act 2018 (UK) (the "**DPA**") and the General Data Protection Regulation (EC) (the "**GDPR**"); and

(b) in the case of Internal Affairs: The Unsolicited Electronic Messages Act 2007 (NZ) (the "Act").

1.7 This MoU sets out the legal framework for information sharing, but it is for each Participant to determine for themselves that any proposed disclosure is compliant with the law applicable to them.

2. The role and function of the Information Commissioner

2.1 The Commissioner is a corporation sole appointed by Her Majesty the Queen under the Data Protection Act 2018 (UK) to act as the UK's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

2.2 The Commissioner is empowered to take a range of regulatory action for breaches of the following legislation (as amended from time to time):

(a) The Data Protection Act 2018 (UK) ("DPA");

(b) The General Data Protection Regulation (EC)("GDPR");

(c) The Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK) ("PECR");

(d) The Freedom of Information Act 2000 (UK) ("FOIA");

(e) The Environmental Information Regulations 2004 (UK) ("EIR");

(f) The Environmental Protection Public Sector Information Regulations 2009 (UK)("INSPIRE Regulations");

(g) The Investigatory Powers Act 2016 (UK);

(h) The Re-use of Public Sector Information Regulations 2015 (UK);

(i) The Enterprise Act 2002 (UK);

(j) The Security of Network and Information Systems Directive ("NIS Directive"); and

(k) The Electronic Identification, Authentication and Trust Services Regulation (EC)("EIDAS").

2.3 The Commissioner has a broad range of statutory duties, including monitoring and enforcement of data protection laws and electronic messaging regulations, and promotion of good practice and adherence to the data protection obligations by those who process personal data. These duties sit alongside those relating to the other enforcement regimes.

2.4 The Commissioner's regulatory and enforcement powers include:

(a) conducting assessments of compliance with the DPA, GDPR, PECR, EIDAS, the NIS Directive, FOIA and EIR;

(b) issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;

(c) issuing enforcement notices, warnings, reprimands, practice recommendations and other orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of data protection legislation and other information rights obligations;

(d) administering fines by way of penalty notices in the circumstances set out in section 152 of the DPA;

(e) administering fixed penalties for failing to meet specific obligations (such as failing to pay the relevant fee to the Commissioner);

(f) issuing decision notices detailing the outcome of an investigation under FOIA or EIR;

(g) certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under FOIA or EIR; and

(h) prosecuting criminal offences before the Courts.

2.5 Regulation 31 of PECR, as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (UK), also provides the Commissioner with the power to serve enforcement notices and issue monetary penalty notices as above to organisations who breach PECR. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of PECR,

including automated telephone calls made without consent, live telephone calls which have not been screened against the Telephone Preference Service, and unsolicited electronic messages (Regulations 19, 21 and 22 of PECR respectively).

3. ROLE AND FUNCTIONS OF THE NEW ZEALAND DEPARTMENT OF INTERNAL AFFAIRS

3.1 The New Zealand Department of Internal Affairs (Internal Affairs), through the Digital Safety Directorate of its Regulatory Services Group is responsible for the enforcement of the Unsolicited Electronic Messages Act 2007 (NZ), in accordance with section 20 of that Act.

3.2 The Unsolicited Electronic Messages Act 2007 (the Act) prohibits the sending of unsolicited commercial electronic messages (email, SMS text, instant messages and facsimile) with a New Zealand link. It requires commercial electronic messages to include accurate information about the person who authorised the sending of the message, and a functional unsubscribe facility. The Act also prohibits address-harvesting software or a harvested-address list from being used in connection with sending unsolicited commercial electronic messages.

3.3 Internal Affairs may investigate, and take enforcement action in relation to, an alleged civil liability event. Civil liability events may result in a formal warning, civil infringement notice, an enforceable undertaking, or an application for pecuniary penalty to the Courts. Internal Affairs may also apply for, and execute, a search warrant in relation to suspected civil liability events.

4. SCOPE OF CO-OPERATION

4.1 The Participants acknowledge that it is in their common interest to collaborate in accordance with this MoU, in order to:

(a) Ensure that the Participants are able to deliver the regulatory cooperation necessary to underpin their data-based economies and protect the fundamental rights of citizens of the United Kingdom and New Zealand respectively, in accordance with the applicable laws of the Participants' respective jurisdictions;

(b) Cooperate with respect to the enforcement of their respective applicable laws relating to electronic messaging;

(c) Keep each other informed of developments in their respective countries having a bearing on this MoU; and

(d) Recognise parallel or joint investigations or enforcement actions by the Participants as priority issues for co-operation.

4.2 For this purpose, the Participants may jointly identify one or more areas or initiatives for cooperation. Such cooperation may include:

(a) sharing of experiences and exchange of best practices on electronic messaging policies, education and training programmes;

(b) implementation of joint research projects;

(c) exchange of information (excluding personal data) involving potential or on-going investigations of organisations in the respective jurisdictions in relation to a contravention of electronic messaging regulations;

(d) joint investigations into cross border incidents concerning unsolicited electronic messages involving organisations in both jurisdictions (excluding sharing of personal data);

(e) convening bilateral meetings annually or as mutually decided between the Participants; and

(f) any other areas of cooperation as mutually decided by the Participants.

4.3 This MoU does not impose on either the Commissioner or Internal Affairs any obligation to co-operate with each other or to share any information. Where a Participant chooses to exercise its discretion to co-operate or to share information, it may limit or impose conditions on that request. This includes where (i) it is outside the scope of this MoU, or (ii) compliance with the request would breach the Participant's legal responsibilities

5. NO SHARING OF PERSONAL DATA

5.1 The Participants do not intend that this MoU shall cover any sharing of personal data by the Participants.

5.2 If the Participants wish to share personal data, for example in relation to any cross border incidents concerning unsolicited electronic messages involving organisations in both jurisdictions, each Participant shall consider compliance with its own applicable data protection or privacy laws, which may require the Participants to enter into a written agreement or arrangement regarding the sharing of such personal data or seek an exemption under law.

6. INFORMATION SHARED BY THE COMMISSIONER

6.1 Section 132(1) of the DPA states that the Commissioner can only share certain information if she has lawful authority to do so, where that information has been obtained, or provided to, the Commissioner in the course of, or for the purposes of, discharging the Commissioner's functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources.

6.2 Section 132(2) of the DPA sets out the circumstances in which the Commissioner will have the lawful authority to share that information. Of particular relevance when the Commissioner is sharing information with Internal Affairs are the following circumstances, where:

(a) The sharing is necessary for the purpose of discharging the Commissioner's functions (section 132(2)(c)); and

(b) The sharing is necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person (section 132(2)(f)).

6.3 Before the Commissioner shares such information with Internal Affairs, the Commissioner may identify the function of Internal Affairs with which that information may assist and assess whether that function of Internal Affairs could reasonably be achieved without access to the particular information in question.

6.4 The Commissioner may choose to share certain information with Internal Affairs only if Internal Affairs agrees to certain limitations on how it may use that information.

7. INFORMATION SHARED BY INTERNAL AFFAIRS

7.1 The Privacy Act 1993 and the Privacy Principles in New Zealand promote and protect individual privacy, governing the collection, access, use and disclosure of personal information.

7.2 Privacy principle 11 (e) states that "an agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds (...) that non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including prevention, detection, investigation, prosecution, and punishment of offence (...)". [] Information may also be shared where an agency has an approved information sharing agreement (AISA) under the Privacy Act or has an exemption issued by the Privacy Commissioner under that Act.

8. SECURITY AND DATA BREACH REPORTING

8.1 Appropriate security measures shall be agreed by the Participants to protect information transfers in accordance with the sensitivity of the information and any security classification that is applied by the sender agency.

8.2 Where confidential material is shared between the Participants it will be marked with the appropriate security classification.

8.3 Where one Participant has received information from the other, it will consult with the other Participant before sharing or disclosing the information to a third party or using the information in an enforcement proceeding or court case.

8.4 Where confidential material obtained from, or shared by, the originating Participant is wrongfully disclosed or wrongfully used by the receiving Participant, the receiving Participant will bring this to the attention of the originating Participant without delay.

9. REVIEW OF THIS MoU

9.1 The Commissioner and Internal Affairs will monitor the operation of this MoU and review it biennially, or sooner if either Participant so requests.

9.2 Any issues arising in relation to this MoU will be notified to the designated point of contact for each Participant.

9.3 This MoU may only be amended by the Participants in writing and signed by each Participant.

10. NON-BINDING EFFECT OF THIS MoU AND DISPUTE SETTLEMENT

10.1 This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the Commissioner or Internal Affairs.

10.2 The Participants will settle any disputes or disagreement relating to or arising from this MoU amicably through consultations and negotiations in good faith without reference to any international court, tribunal or other forum.

11. DESIGNATED CONTACT POINTS

11.1 The following persons shall be the designated contact points for the Participants for matters under this MoU:

Information Commissioner's Office	**New Zealand Department of Internal Affairs**
Name: Adam Stevens Designation: Head of Intelligence	Name: Jolene Armadoros Designation: Digital Safety Director

11.2 The above individuals will maintain an open dialogue between each other in order to ensure that this MoU remains effective and fit for

purpose. They will also seek to identify any difficulties in the working relationship, and proactively seek to minimise the same.

11.3 Each Participant may change its designated contact point for the purposes of this MoU upon notice in writing to the other Participant.

Signatories:

Stephen Eckersley **Director of Investigations**	**Jolene Armadoros** **Digital Safety Director**
[redacted]	[redacted]
Date: 16 December 2019	Date: 6-1-2020